

**Before the Federal Communications Commission**

---

*IN RE*  
**RULES AND REGULATIONS**  
**IMPLEMENTING THE TRUTH IN CALLER ID ACT OF 2009**

---

*ON NOTICE OF PROPOSED RULEMAKING*

---

**COMMENTS OF THE**  
**NATIONAL EMERGENCY NUMBER ASSOCIATION**

---

**TELFORD E. FORGETY, III**  
*Attorney*  
*Director of Government Affairs*

*NATIONAL EMERGENCY*  
*NUMBER ASSOCIATION*  
*4350 N. Fairfax Dr., Ste. 750*  
*Arlington, VA 22203-1695*  
*(703) 812-4600*

---



The National Emergency Number Association (“NENA”) respectfully submits the following comments in response to the *Notice of Proposed Rulemaking* adopted by the Commission on March 9<sup>th</sup>, 2011 in this proceeding.

## COMMENTS

When Congress passed the Truth in Caller ID Act of 2009, it had the foresight to specifically prohibit the spoofing of Automatic Number Identification systems and to inquire into foreseeable advances in technology that may require the adoption of new laws to ensure the continued security of our nation’s communications systems. As the Commission moves to implement the Act, it is imperative that it do so with an eye toward the rapidly advancing state of emergency communications systems in particular. Next Generation 9-1-1 (“NG9-1-1”) will enable the public to seek emergency services through a variety of communications methods including IP-based voice, video, and text. These novel services will bring with them new challenges as we move beyond the calling party identification schemes inherited from the architecture of legacy wireline networks. It is therefore important that the Commission ensure that nothing in its rules unnecessarily limits the operation of such services purely out of deference to the *status quo*.

More immediately, however, it is imperative that the Commission adopt strong rules prohibiting the harmful manipulation of calling party number services including Automatic Number Identification. Such manipulation has a particularly detrimental impact upon public safety, and NENA urges the Commission to bear this in mind as it considers the enforcement framework for the rules adopted in this proceeding.

### **I. The Commission should read the term “IP-Enabled Voice Service” broadly.**

NENA has previously commented on the difficulties that result from the Commission’s current definition of “inter-connected VoIP service[s]” in the joint Wireless Location

Accuracy and VoIP proceeding, Docket No. 05-197/07-14. To avoid belaboring our previous arguments, we merely reiterate the need for VoIP rules that look to the substance rather than the marketing of VoIP services, and commend to the Commission's consideration the reasonable and logical proposal submitted by the Department of Justice as one example of a workable definition of "IP-Enabled Voice Service."

## **II. The definition of Automatic Number Identification should be expansive.**

NENA urges the Commission to adopt a definition of ANI that encompasses the delivery of charge party numbers from IP-Enabled Voice Service providers in order to ensure that these services – which may subject a potential spoofer to fewer obstacles – do not become a weapon-of-choice by virtue of their exclusion. Further, we recommend that Commission minimize the potential for an internal statutory conflict by reading the definition of Caller Identification Information *noscitur a sociis* with the succeeding definition of Caller Identification Service and concluding that the absence of a specific reference to ANI in the former was not intended to convey meaning. Finally, we largely agree with the definition of Caller Identification Information proposed by the Commission, but urge the Commission to include the Jurisdiction Information Parameter within that definition to ensure this data is available to present and/or future emergency call routing systems.

## **III. Special presumptions should apply to spoofing directed to public safety answering points and other emergency service providers.**

### **A. *Spoofing ANI or pANI services should be irrebuttably presumed to "cause harm."***

Automatic Number Identification and Pseudo Automatic Number Identification are foundations of the emergency services routing infrastructure in the United States. Unlike other calling party number services, both ANI and

pANI derive their data exclusively from information maintained in the records of the originating service provider. Therefore these services are not subject to manipulation by callers in the ordinary course of using a telecommunications service, interconnected VoIP service, or mobile telephony service. Consequently, NENA considers the probability that individual could successfully spoof ANI or pANI on a reproducible basis to be negligible. However, because the consequences of such spoofing would be particularly great, we consider it imperative that the Commission adopt a stern posture toward such an offense.

If an individual managed to successfully spoof an ANI service, the consequences to public safety would be three-fold. First, such an individual could conceal his or her identity, making it difficult for law enforcement agencies and prosecutors to interdict harassing, prank, or other unlawful 9-1-1 calls. Second, such an individual could conceal his or her location, since Automatic Location Information (ALI) databases rely on ANI information to deference the location of a caller on the basis of the ALI record passed with a 9-1-1 call. This would further complicate efforts to interdict harmful or abusive 9-1-1 calls. Finally, if an individual could successfully spoof an ANI service, such an individual could tie up precious public safety response capacity by initiating spoofed calls designed to cause the dispatch of responder units to locations where no emergency is actually at hand.

Because of the great lengths to which an individual would have to go in order to successfully spoof an ANI system and the potential for grave harm that could result from such an exploit, NENA recommends that the Commission apply an irrebuttable presumption of harm whenever an ANI service is spoofed. Such a presumption would do much to deter the manipulation of ANI services, or insider activities needed to carry out such a scheme.

***B. Spoofing Caller ID when calling 9-1-1 or other emergency service numbers should be rebuttably presumed to “cause harm.”***

While ANI and pANI are the most widespread caller identification services relied upon by public safety answering points, they are not the only such services. More than 40 years after the first 9-1-1 call was placed there remain areas of the United States that still lack enhanced or even *basic* 9-1-1 services. In those areas, public safety answering points or individual emergency response agencies can use consumer-grade calling party number identification services to obtain at least some information (such as name and call-back number) from an individual requesting emergency services. Even in areas with more advanced E9-1-1 services, such caller ID information may still be presented to telecommunicators as an additional source of information about a caller and the caller’s whereabouts.

These consumer-grade services are not based on exclusively internal carrier-network information characteristic of ANI and pANI, however. As a result, they are subject to the full panoply of spoofing strategies identified by Congress and undoubtedly to others. Unlike ANI and pANI, however, consumer-grade calling party number services can be manipulated for legitimate business or security reasons. Consequently, an irrebuttable presumption of harm would not serve the public interest. But all of the harms identified above in regard to ANI spoofing can result equally from other forms of caller ID spoofing, particularly when the target PSAP or public safety agency has no 9-1-1 service or only basic 9-1-1 service. NENA therefore considers it appropriate that the Commission apply a rebuttable presumption of harm whenever a caller knowingly causes a caller identification service to transmit misleading or inaccurate caller identification information to a 9-1-1 system or public safety agency. By allowing an accused spoofer to rebut the presumption of harm, the Commission can increase the deterrent effect of the prohibitory rule while lessening the probability that legiti-

mate manipulation of caller ID services will result in undeserved enforcement action.

## CONCLUSION

This NPRM represents a critical opportunity to safeguard the integrity of vital public safety information sources. In order to ensure the speed and efficiency of emergency response services, the Commission should adopt broad definition so IP-Enabled Voice Services and Automatic Number Identification and establish an enforcement framework that represents the severity of the harms that spoofing can impose on the safety of the public.

TELFORD E. FORGETY, III  
*Attorney*

APRIL 2011